UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/693,149 | 10/23/2003 | Frederick S. M. Herz | REFH-0163 | 1678 |

23377 7590 02/02/2010
WOODCOCK WASHBURN LLP
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

| EXAMINER | |
|---|---|
| WYSZYNSKI, AUBREY H | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2434 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 02/02/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|  |  |  |
|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/693,149 | **Applicant(s)**<br>HERZ, FREDERICK S. M. |
|  | **Examiner**<br>AUBREY H. WYSZYNSKI | **Art Unit**<br>2434 |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on _26 October 2009_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) _2-14 and 16-21_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _2-14 and 16-21_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _23 October 2003_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

## DETAILED ACTION

1. The response of 10/26/09 was received and considered.

2. Claims 1 and 15 are canceled.

3. Claims 2-14 and 16-21 are pending.

### *Response to Arguments*

4. Applicant's arguments filed 10/26/09 have been fully considered but they are not persuasive.

Applicant argues that each sensor 104 of Anderson lacks the claimed “data collection means”, “analyzing means” and “comparing means”. However, this argument is moot because the Directors 102 (fig. 1) of Anderson performs the “data collection means”, “analyzing means” and “comparing means” wherein the examiner is equating the Directors 102 to the claimed "agents". Please also note paragraph 0022 of the specification that teaches “In particular, the present invention may also be practiced with one or more directors 102. When more than one director 102 is employed, each director 102 may be assigned responsibility for a subset of sensors 104a-104n, and the directors 102 may relate to each other in a master/slave relationship, with one of the directors 102 serving as the "master" (and the others as "slave"), or as peers to one another or organized into an hierarchy, to collective discharge the `responsibilities described below.”` Please see the rejection below for further clarification.

5. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2-14 and 16-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson et al., US 2003/0002436 and further in view of Lin et. al., US 6,405,250.

Regarding claims 2 and 18, Anderson discloses a system that detects the state of a computer network, comprising:

agents (fig. 1, Director 102 and ¶0022, more than one Director may be employed) disposed in said computer network (fig. 1 network 112) each said agent comprising:

data collection means for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network (¶0023, director 102 activates an initial subset of sensors 104a-104n to monitor and collect descriptive data for network traffic routed over the network link of interest and/or related links, fig, 2, block 202, and fig. 1, client network nodes 108);

means responsive to the data from the data collection means for analyzing said data to develop activity models representative of activities of said network in a normal state and activities of said network in an abnormal state (¶0024 and fig. 2, block 204); and

means for comparing collected data to said activity models to determine whether said computer network is in said normal state or said abnormal state at different times and to dynamically update said activity models (¶0025-0026 and fig. 2, block 206 and ¶0040), wherein said analyzing means performs a pattern analysis on the collected data and said comparing means compares the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network (fig. 2, block 208, If additional monitoring or data collection is "preferred", director 102 launches additional selected ones of sensors 104a-104n to perform the additional monitoring to collect additional data to confirm that indeed the network link of interest is being misused and fig. 5, step 506-508 and ¶0022).

Anderson lacks or does not expressly disclose developing activity models representative of activities of said network in a normal state and activities of said network in an abnormal state at different times and to dynamically update said activities models. However, Lin discloses developing activity models representative of activities of said network of said network in a normal state and activities of said network in an abnormal state (fig. 2, state 1, normal state and fig. 5, state 501, normal, and state 511, state changed) at different times and to dynamically update said activities models (col. 1, lines 30-42). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Anderson with the activity models of Lin in order to monitor the health of the network, as taught by Lin (col. 1, lines 30-42).

Regarding claim 3, Anderson as modified above discloses the system of claim 2, wherein said agents comprise a plurality of distributed agents (¶0022, one or more Directors may be employed).

Regarding claim 4, Anderson as modified above discloses the system of claim 2, wherein said data collection means collects data representative of operation of said computer network, including respective nodes in said computer network, said data relating to communications, internal and external accesses, code execution functions, and/or network resource conditions of respective nodes in said computer network (¶0025 and abstract).

Regarding claim 5, Anderson as modified above discloses the system of claim 2. Lin further discloses wherein said activity models characterize conditions within said computer network including behaviors, events, and/or functions of respective nodes of said computer network, said behaviors representative of said normal state and one or more abnormal states representative of suspicious activity in said computer network (fig. 3, network wide activity model).

Regarding claim 6, Anderson as modified above discloses the system of claim 2, further comprising means for characterizing the state of the computer network and identifying any potential threats based on said collected data (fig. 2, step 206, detect if network link is being misued).

Regarding claim 7, Anderson as modified above discloses the system of claim 6, wherein said characterizing means further recommends remedial repair and/or recovery strategies to isolate and/or neutralize the identified potential threats to the computer system (fig. 2, steps 214-218, determine regulation).

Regarding claim 8, Anderson as modified above discloses the system of claim 2, wherein respective agents are connected by redundant communications connections (fig. 1, sensors 104 and routing devices 106).

Regarding claim 9, Anderson as modified above discloses the system of claim 2, wherein each agent is implemented in redundant memory and hardware that is adapted to be insulated from infected components of said computer network (fig. 5, step 510).

Regarding claim 10, Anderson as modified above discloses the system of claim 2, wherein the agents are disposed in a hierarchical structure whereby communications from bottom level agents to agents at higher levels in the hierarchy are limited (¶0022 and fig. 1).

Regarding claim 11, Anderson as modified above discloses the system of claim 2, further comprising means for predictively modeling the behavior of said computer network based on sequentially occurring behavior patterns in the data collected by said data collection means (¶0040).

Regarding claim 12, Anderson as modified above discloses the system of claim 2. Lin further discloses wherein said comparing means comprises means for pattern matching collected data with data in said activity models to determine a closest activity model based upon similarity of the data in each data model with the collected data (fig. 3, state of the network wide model).

Regarding claim 13, Anderson as modified above discloses the system of claim 2, wherein the collected data represents actions of a virus, system responses to actions of a virus, actions of a hacker, system responses to actions of a hacker, threats directed to discrete objects in said computer network, and/or potential triggers of a virus or threat to said computer network (¶0032, network misuse).

Regarding claim 14, Anderson as modified above discloses the system of claim 2. Lin further discloses wherein said analyzing means for each agent filters and analyzes received data and dynamically redistributes the analyzed and filtered data to other agents associated with said each agent (col. 6, lines 2-11).

Regarding claim 16, Anderson as modified above discloses the system of claim 2, wherein the comparing means compares names and email addresses in said collected data against known criminal, hoaxsters and/or aliases for known criminals and hoaxsters (¶0005).

Regarding claim 17, Anderson as modified above discloses the system of claim 2, further comprising a trusted server that receives attack data from a plurality of agents identifying abnormal states indicative of a network attack, said trusted server gathering the attack data and sending warnings to selected nodes in said computer network (fig. 6, alert).

Regarding claim 19, Anderson as modified above discloses the method of claim 18, wherein the agents report any suspicious activity that exceeds a suspicion threshold (¶0032, user define threshold).

Regarding claim 20, Anderson as modified above discloses the method of claim 19, wherein the agents transmit said analyzed data in order to determine an origin of the suspicious activity in the computer network (¶0032).

Regarding claim 21, Anderson as modified above discloses the method of claim 20, further comprising scanning said analyzed data for patterns and comparing said patterns to data representative of patterns of known threats to said computer network for identification of said suspicious activity (¶0032).

## *Conclusion*

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. The examiner has pointed out particular references contained in the prior art of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as

well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AUBREY H. WYSZYNSKI whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aubrey H Wyszynski/
Examiner, Art Unit 2434
/Kambiz  Zand/

Supervisory Patent Examiner, Art Unit 2434